

**IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA  
ALEXANDRIA DIVISION**

UNITED STATES OF AMERICA

v.

ZIGUANG LI,

*Defendant.*

**UNDER SEAL**

Case No. 1:24-mj-188

18 U.S.C. § 1956(h)  
Conspiracy to Commit Concealment Money  
Laundering

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT  
AND ARREST WARRANT**

I, Special Agent Adam Cowan of the Department of the Treasury, being first duly sworn,  
hereby depose and state as follows:

**INTRODUCTION**

1. Based upon the facts set forth in this affidavit, there is probable cause to believe that **Ziguang LI** (the “**TARGET**”), and others, have committed violations of 18 U.S.C. §1956(h) (Conspiracy to Commit Concealment Money Laundering). This affidavit is made in support of a Criminal Complaint and Arrest Warrant for **Ziguang LI**.

**AGENT BACKGROUND**

2. I am a Senior Special Agent with the Department of the Treasury, Treasury Inspector General for Tax Administration (“TIGTA”) where I have been employed since August of 2019. As a TIGTA Special Agent, I am authorized to conduct criminal and other investigations arising under the laws of the United States and regulations administered by the Department of the Treasury and the Internal Revenue Service (“IRS”); to require and receive information relating to such laws and regulations; to carry firearms; to serve subpoenas and

summonses; and to execute and serve search and arrest warrants. I am currently assigned to TIGTA's Cybercrime Investigations Division ("CCID") where I primarily investigate fraud and other criminal activity involving government computer systems. Before my employment with TIGTA, I was a Supervisory Marine Interdiction Agent with U.S. Customs and Border Protection ("CBP"), Air and Marine Operations ("AMO"), where my responsibilities included detecting and investigating violations of federal laws. I am a graduate of the Criminal Investigator Training Program ("CITP") and I have received additional training in cyber investigations, cyber incident response, and digital forensics. I have participated in numerous financial crime investigations and have experience analyzing financial documents, interviewing suspects and witnesses, conducting physical and electronic surveillance, serving search and arrest warrants, and collecting, preserving, and examining physical and electronic evidence. In addition, I have served as the affiant for numerous Criminal Complaints related to financial crime investigations.

3. Through training and experience, I have become familiar with the manner in which various fraud schemes are conducted and the methods by which fraudsters collect, store, and conceal the proceeds of their illegal activities. I am also familiar with the manner in which fraudsters use cellular telephones, encrypted telephone applications (e.g. Telegram), slang filled communications and other means to facilitate their illegal activities and thwart law enforcement investigations.

4. I have personally participated in this investigation and have witnessed many of the facts and circumstances described herein. The information set forth in this affidavit is based on my own personal knowledge, my review of relevant records, reliable information provided to me by other law enforcement officers, and my training and experience. This affidavit is

intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim.

### **SUBJECT OFFENSES**

5. *Conspiracy to Commit Money Laundering.* I know from my training and experience and discussions with federal prosecutors that Title 18, United States Code, Section 1956(h) makes it a crime to conspire to commit money laundering as set forth in Section 1956.

6. *Concealment Money Laundering.* I know from my training and experience and discussions with federal prosecutors that Title 18, United States Code, Section 1956(a)(1)(B) makes it a crime to conduct a financial transaction designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

7. The term “financial transaction” means (A) a transaction which in any way or degree affects interstate or foreign commerce (i) involving the movement of funds by wire or other means or (ii) involving one or more monetary instruments, or (iii) involving the transfer of title to any real property, vehicle, vessel, or aircraft, or (B) a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree. 18 U.S.C. § 1956(c)(4)

8. Wire fraud is a specified unlawful activity. 18 U.S.C. § 1956(c)(7)(A); 18 U.S.C. § 1961(1).

### **BACKGROUND ON THE INVESTIGATION**

9. TIGTA, the United States Postal Inspection Service (“USPIS”), and the Federal Bureau of Investigation (“FBI”) are investigating a wire fraud and money laundering conspiracy

that shows **LI** and other conspired to launder wired funds obtained from victims of a tech support scam.<sup>1</sup> To do so, **LI** and others exploited the IRS's Modernized Internet Employer Identification Number ("Mod IEIN") online portal. Mod IEIN is the IRS system that allows users to register for a unique Employer Identification Number ("EIN") for a business. These transactions are processed at IRS Enterprise Computing Centers located in West Virginia and Tennessee, making each of these transactions an interstate wire communication.

10. The investigation shows that from on or about March 31, 2023 through on or about February 22, 2024, **LI**, and others obtained EINs for various businesses in furtherance of their criminal scheme. These EINs allowed the co-conspirators to open business<sup>2</sup> bank accounts at various financial institutions for the purpose of laundering wired funds obtained through a tech support scam.

11. Through victim interviews and the review of complaints submitted to the Internet Crime Complaint Center ("IC3"),<sup>3</sup> law enforcement has determined that many of these wire

---

<sup>1</sup> From training and experience, I know that tech support scams typically involve a fraudster who impersonates an employee of a legitimate technology company (e.g., Microsoft) and offers to "fix" a non-existent problem on the victim's computer. The fraudster will often trick the victim into (1) giving the fraudster access to the victim's financial accounts (2) installing malicious software on the victim's computer, and/or (3) giving the fraudster remote access to the victim's computer. According to the National Council on Aging's website "In 2020, at least 66% of tech support scam victims were age 60 or older."

<sup>2</sup> From training and experience, I know that fraudsters often prefer business bank accounts for schemes involving high dollar transactions. This is due to the perception that banks apply greater scrutiny to large deposits when they are credited to personal bank accounts.

<sup>3</sup> IC3 is an FBI led program that allows victims of cyber-crime to file formal complaints. These complaints are made available to federal, state, local, or international law enforcement as appropriate.

transfers were the result of a tech support scam targeting older adults. The investigation shows that **LI** directly received proceeds from this fraudulent activity and conducted further financial transactions to conceal the illicit source of these funds. In addition, the investigation shows that **LI** facilitated the transfer of fraud proceeds to bank accounts controlled by a third party in exchange for cryptocurrency.

### **PROBABLE CAUSE**

#### **A. Fictitious Business<sup>4</sup> Kim Fashionable Clothing Inc.**

12. On March 31, 2023, someone logged into the IRS's Mod IEIN online portal from a Queens, New York IP address) and used J.D.'s<sup>5</sup> Social Security Number ("SSN-1") to assign EIN:XX-XXX1373 to the fictitious business Kim Fashionable Clothing Inc of Fairfax, Virginia. On April 18, 2023, a business bank account (account number xxxxxxxx1017) was opened for Kim Fashionable Clothing Inc (EIN: XX-XXX1373) at Bank-1, a financial institution as defined in Title 18, United States Code Section 20, at a location in the Eastern District of Virginia.

13. Kim Fashionable Clothing Inc. has no online presence or physical storefront and does not appear to be engaged in any form of legitimate business. Account number xxxxxxxx1017 was opened by an individual claiming to be J.D., however Bank-1 surveillance

---

<sup>4</sup> Each "fictitious business" set forth in this affidavit appears to be a "shell" company. Shell companies are used for various purposes, including to disguise the true intent and nature of fraud schemes. The use of a shell company also provides a layer of anonymity for the individuals involved in the scheme.

<sup>5</sup> The actual J.D. is a resident of Texas and has no known connections to Queens, New York (where the EIN for Kim Fashionable Clothing Inc was assigned), Fairfax, Virginia, or the email address and phone numbers provided for Kim Fashionable Clothing Inc in bank and IRS records. Law enforcement has interviewed another individual whose identity was been linked to a fictitious businesses utilized in this tech support scam and learned that that individual was a victim of identity theft.

captured images of Individual-1 and Individual-2 conducting cash withdrawals from account number xxxxxxxx1017 on multiple occasions. As explained later, identification documents belonging to J.D. as well as Kim Fashionable Clothing Inc. records were recovered from LI's residence during the execution of a residential search warrant.

14. Between June 5, 2023, and July 13, 2023, Bank-1 account number xxxxxxxx1017 opened in the name of J.D. and Kim Fashionable Clothing Inc. was the beneficiary of six wire transfers (from suspected victims<sup>6</sup>) totaling over \$257,000. These victim-funded wire transfers are the only funds credited to this account (besides the \$100 opening deposit) and include:

- a. A \$23,689.79 wire transfer from Victim-1's Bank-2 account on June 7, 2023.

Bank-2 is a financial institution as defined in Title 18, United States Code Section 20.

- b. A \$58,750.00 wire transfer from Victim-2's Bank-3 account on June 8, 2023.

Bank-3 is a financial institution as defined in Title 18, United States Code Section 20.

15. Victim-1 and Victim-2 subsequently submitted IC3 complaints alleging that the wire transfers from their respective accounts were the result of a tech support scam. According to the IC3 complaints, Victim-1 received a message on their desktop computer stating that their computer was locked due to a hacker and directing them to contact "Microsoft" at the number provided. Victim-2's computer froze and a Microsoft logo appeared along with a 1-800 number

---

<sup>6</sup> Law enforcement has not obtained documentation from all of the suspected victims to confirm that they were victims of the tech support scam. However, based on the victim documentation that has been obtained and the fact that these large wire transfers all originated from personal bank accounts during the same time frame as wire transfers from confirmed victims, law enforcement suspects that each of these individuals fell victim to the tech support scam.

for them to call for assistance. After calling the numbers that appeared on their computers, Victim-1 and Victim-2 were each tricked into conducting the wire transfers from their respective accounts.

16. On June 8, 2023, Bank-1 account number xxxxxxxx1017 initiated a \$48,000.00 wire transfer to account number xxxxxx7970 at Bank-4, a financial institution as defined in Title 18, United States Code Section 20, for the benefit of Staring LLC. On June 9, 2023, account number xxxxxxxx1017 initiated an \$82,000.00 wire transfer to Bank-4 account number xxxxxx7970 for the benefit of Staring LLC. As described in further detail in paragraph 20, Staring LLC is a business registered to **LI**.

17. Further investigation revealed that business bank accounts were opened for Kim Fashionable Clothing Inc. (using the name J.D. and EIN: XX-XXX1373) at other financial institutions, including account number xxxxxx6617 at Bank-5 and account number xxxxxx9228 at Bank-2. As summarized below, these accounts received tech support scam victim funds:

- a. Between June 27, 2023 and June 29, 2023, Bank-5 account number xxxxxx6617 was the beneficiary of seven wire transfers totaling over \$200,000. IC3 complaints were subsequently filed by, or on behalf of, the originators of three of these wire transfers alleging variations of the tech support scam (i.e. the victim's computer was frozen and they contacted the number for "Microsoft" that appeared on their screen, or the victim's computer was comprised and the wire transfer was sent without the victim's authorization).
- b. On June 12, 2023, Bank-2 account number xxxxxx9228 received a \$50,000 wire transfer from Victim-3's Fidelity Investments account. Victim-3 subsequently filed an IC3 complaint alleging a tech support scam. In the IC3 complaint,

Victim-3 stated that they received a Windows firewall alert while they were logging into their Fidelity Investments account and contacted “Microsoft” at the number that appeared on his screen.

18. On August 22, 2023, USPIS interviewed Victim-3 (identified as an 80-year-old resident of Michigan) and verified that the wire transfer from Victim-3’s Fidelity Investments account to Bank-2 account number xxxxxx9228 was the result of a tech support scam.

**B. Fictitious Business Coco Love Nail Art Wholesale Inc**

19. On April 6, 2023, Bank-6 account number xxxxxxx8875 was opened for Coco Love Nail Art Wholesale Inc (EIN: XX-XXXX943) at a location in the Eastern District of Virginia. Similar to Kim Fashionable Clothing Inc, Coco Love Nail Art Wholesale Inc has no online presence or physical storefront and does not appear to be engaged in any form of legitimate business. Between May 31, 2023 and June 1, 2023, Bank-6 account number xxxxxxx8875 was the beneficiary of two wire transfers (from suspected victims) totaling over \$110,000. On June 1, 2023, Bank-6 account number xxxxxxx8875 attempted to initiate a \$16,500 wire transfer to Bank-4 account number xxxxx7939 for the benefit of Immortal Manufacturing LLC. As described in further detail in paragraph 20, Immortal Manufacturing LLC is another business registered to **LI**.

**C. LI owns Staring LLC and Immortal Manufacturing LLC**

20. On June 7, 2022, **LI**’s name and Taxpayer Identification Number (“TIN”) logged into Mod IEIN and assigned EIN 88-2687771 to the business Immortal Manufacturing LLC. Also on June 7, 2022, Immortal Manufacturing LLC (registered agent and managing member **Ziguang LI**) filed Articles of Organization with the Nevada Secretary of State.



21. On February 7, 2023, **LI**'s name and TIN logged into Mod IEIN and assigned EIN 92-2198780 to the business Staring LLC. Also on February 7, 2023, Staring LLC (registered agent and managing member **Ziguang LI**) filed Articles of Organization with the Nevada Secretary of State.

#### **D. LI'S BANK ACCOUNTS**

22. On May 17, 2023, **LI** opened Bank-4 account number xxxxx7939 for Immortal Manufacturing LLC (EIN: XX-XXX7771) at a location in the District of Nevada. According to the signature card for Bank-4 account number xxxxx7939, Immortal Manufacturing LLC's purported nature of business is "diamond trade."

23. On May 30, 2023, **LI** opened Bank-4 account number xxxxxx7970 for Staring LLC (EIN: XX-XXX8780) at a location in the District of Nevada. According to the signature card for Bank-4 account number xxxxx7970, Staring LLC's purported nature of business is "computer software maintenance, diamond trade & others."

24. Between May 22, 2023 and June 5, 2023, Bank-4 account number xxxxx7939 received five wire transfers totaling over \$79,000. Three of these wire transfers originated from the Bank-5 account of a business identified as Above and Beyond Heating Corp of Annandale, Virginia.

25. A review of IC3 complaints identified a complaint filed by Arizona Adult Protective Services on behalf of Victim-4. Victim-4 (identified as an over 60- year-old resident of Arizona) alleged wired \$24,500 to Above and Beyond Heating Corp's Bank-5 account as the result of a tech support scam. Accordingly, law enforcement believes that Above and Beyond Heating Corp is another fictitious business that is being utilized as part of this scheme to defraud.

26. Between June 5, 2023 and June 9, 2023, Bank-4 account number xxxxxx7970 received four wire transfers totaling over \$144,000:

- a. Two (2) wire transfers originated from the Bank-1 account of Kim's Fashionable Clothing Inc (referenced in paragraph 16),
- b. One (1) wire transfer originated from the Bank-5 account of Kim Fashionable Clothing Inc (referenced in paragraph 17), and
- c. One (1) wire transfer originated from the Bank-5 account of Above and Beyond Heating Corp.

27. On June 13, 2023, Bank-7 check number 8807 (\$38,286) was deposited into Bank-4 account number xxxxxx7970. This check was purchased by Global Auto Repair LLC of Irwindale, California and made payable to Staring LLC. A review of IC3 complaints identified a complaint from Victim-5 who stated that they were the target of a tech support scam on May 15, 2023. According to the complaint, the fraudsters directed Victim-5 to wire \$48,380 to the Bank-5 account of Global Auto Repair LLC. Victim-5 realized they were being scammed and refused to wire the funds. Based on this attempt to defraud, law enforcement believes that Global Auto Repair LLC is another fictitious business that is being utilized as part of this scheme.

28. On June 14, 2023, Bank-1 informed Bank-4 that the funds underlying the wire transfers on June 8, 2023 and June 9, 2023, from Kim Fashionable Clothing Inc to Staring LLC were unauthorized and the wire transfers involved funds allegedly obtained through fraud.

29. Bank-4 subsequently contacted **LI**, who claimed that the wire transfers from Kim Fashionable Clothing Inc were payment for the purchase of diamonds from Staring LLC. **LI** also claimed to have mailed diamonds to Kim Fashionable Clothing Inc and presented a United States Postal Service ("USPS") mailing label to Bank-4 as proof. Although Staring LLC is

located in the District of Nevada and Kim Fashionable Clothing is located in the Eastern District of Virginia, the USPS tracking information showed that the purported diamond shipment originated from an address in Elkins Park, Pennsylvania and was delivered to an address in Flushing, New York. According to Bank-4 records, **LI** also stated that he did not know the sender listed on mailing label for the purported diamond shipment.

*Bank-4 Money Laundering Activity*

30. The transactions after **LI**'s Staring LLC's Bank-4 account number xxxxxx7970's receipt of two victim-funded wire transfers from Kim Fashionable Clothing Inc.'s Bank-1 account number xxxxxxxx1017 opened in the name of J.D. and for Kim Fashionable Clothing (referenced in paragraph 12) demonstrate the rapid movement of funds commonly associated with money laundering.

31. According to Bank-4 records, **LI**'s Staring LLC's Bank-4 account number xxxxxx7970 received a \$48,000 wire transfer from Kim Fashionable Clothing Inc. on June 8, 2023 at 3:10 pm and a \$82,000 wire transfer from Kim Fashionable Clothing Inc. on June 9, 2023 at 9:32 am. On June 9, 2023 at 12:16 pm, **LI**'s Bank-4 account number xxxxxx7970 initiated a \$15,000 wire transfer to the Bank-5 account of a business identified as BTX Group LLC. On June 9, 2023 at 1:55 pm Bank-4 account number xxxxxx7970 initiated a \$73,000 wire transfer to the Bank-5 account of BTX Group LLC. This rapid series of transactions involving funds derived from victims of a tech support scam appears to have been conducted in an attempt to conceal the illicit source of the funds and/or prevent the financial institutions from freezing the accounts and recalling the funds.

*Other Bank Accounts*

32. In addition to opening accounts for Staring LLC and Immortal Manufacturing LLC at Bank-4, **LI** also opened accounts for Staring LLC at Bank-8 and Bank-9:

- a. Between May 16, 2023, and May 18, 2023, **LI's** Staring LLC account at Bank-8 received seven wire transfers totaling over \$100,000 and two check deposits totaling over \$50,000. On June 21, 2023, Bank-8 recalled all funds in **LI's** Staring LLC account and administratively closed the account.
- b. Between March 28, 2023 and June 22, 2023, **LI's** Staring LLC account at Bank-9 received eight wire transfers from fictitious business linked to the tech support.

33. In total, the investigation shows that **LI's** bank accounts (at Bank-4, Bank-8, and Bank-9) received over \$400,000 from fictitious businesses directly linked to the tech support scam. Funds derived from the tech support scam account for the vast majority of the funds deposited into **LI's** accounts. This total does not include funds derived from the tech support scam that **LI** attempted to launder through the bank accounts of third parties in exchange for crypto currency (as detailed in paragraphs 40 and 41).

#### **E. Google Search Warrant and Returns**

34. On December 15, 2023, I obtained a search warrant for various Google Accounts implicated in the foregoing scheme. *See In re Google Accounts*, 1:23-SW-742-JFA. A preliminary review of these accounts revealed information further implicating **LI**, to include:

- a. A May 31, 2023 email from Bank-4 regarding a \$49,500 wire transfer from Above and Beyond Heating Corp for the benefit of **LI's** business Immortal Manufacturing LLC.
- b. A June 9, 2023 email from Bank-4 regarding an \$82,000 wire transfer from Kim Fashionable Clothing Inc for the benefit of **LI's** business Staring LLC. The originator to beneficiary information in this email states that the purpose of this

wire is POP (i.e., Point of Purchase) GOODS and not diamonds or jewelry as

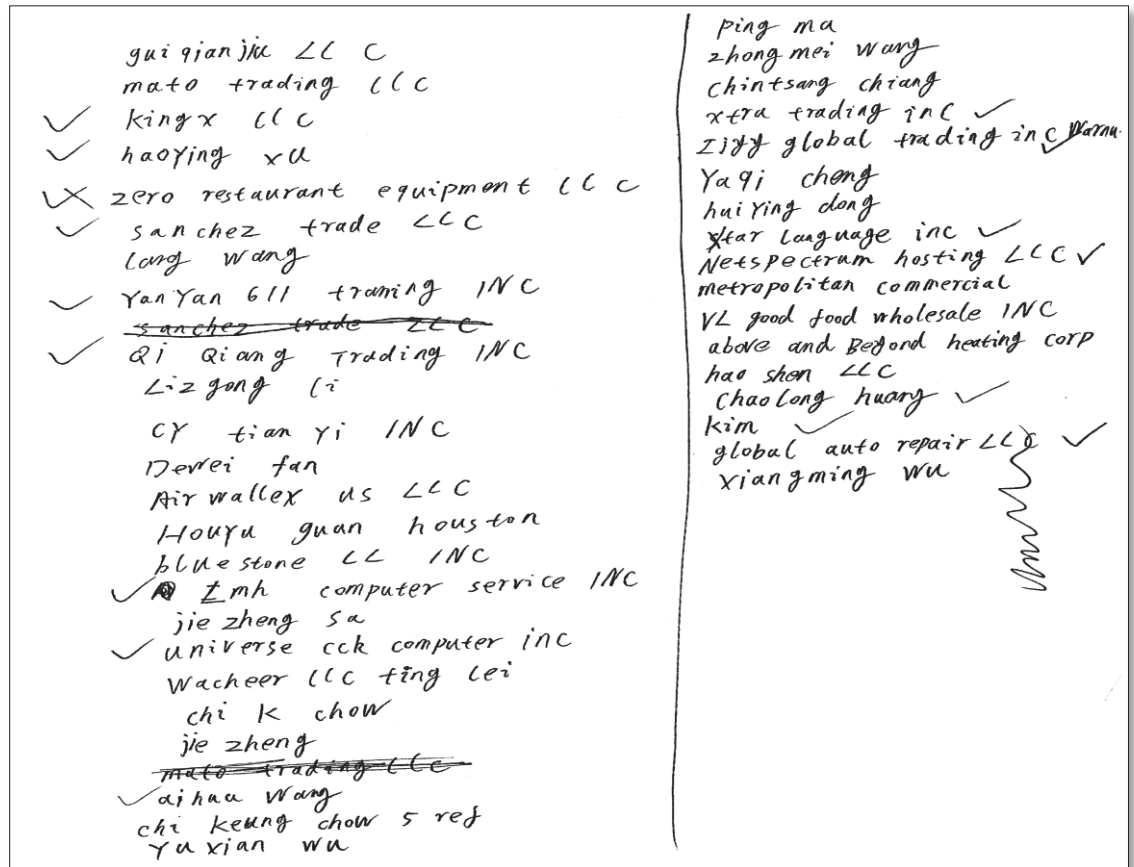
**Ziguang LI** allegedly told Bank-4.

**F. The Search of LI's Residence connects him to Kim Fashionable Clothing, stolen J.D. identification, and the broader tech support scam.**

35. On February 22, 2024, TIGTA and USPIS executed search warrants (Case No. 2:24-mj-159-DJA and Case No. 2:24-mj-160-DJA) on **LI's** residence in the District of Nevada. The search of **LI's** residence resulted in the seizure of evidence further corroborating **LI's** involvement in the fraud scheme described in this affidavit. Some of this evidence is summarized below:

- a. Business documents and bank statements verifying **LI's** ownership of Staring LLC, Immortal Manufacturing LLC, and other suspected fictitious business.

- b. A handwritten list of suspected fictitious businesses. This list (which includes many of the businesses previously referenced in this affidavit) is displayed below:



- c. A stack of printed documents which appear to be “work kits”<sup>7</sup> for approximately 20 suspected fictitious businesses (including many of the fictitious businesses previously referenced in this affidavit). The contents of the Kim Fashionable Clothing Inc work kit are described in detail below:

<sup>7</sup> In fraud schemes, a “work kit” is a set of documents that the fraudster uses to open fraudulent bank accounts and/or conduct or monitor transactions in the fraudulently opened accounts. Work kits typically include stolen or synthetic identity information and fictitious business documents. In my training and experience, work kits are typically transmitted electronically between co-conspirators.

- i. A document (in Chinese and English) containing detailed information about Kim Fashionable Clothing Inc and Bank-1 account number xxxxxxxx1017 (including SSN-1 which was used to obtain the EIN for Kim Fashionable Clothing Inc as described in paragraph 12). An image of this document is displayed below:

	1:注册人/公司类型: INC
	2:法律实体名称/自然人名称: Kim fashionable clothing INC
	3:公司成立国家: USA
	4:公司注册日期: 03/31/2023
	5:公司是否受任何政府机构监管: 否
	6:注册人和其他股东是否曾宣告破产: 否
	如果有, 请解释
	7:注册人和其他股东是否是政治公众人物 : 否
	8:公司是否在美国注册为金融实体 : 否
	9:公司是掉期交易商么?: 否
	<b>信息</b>
	1:公司名称: Kim fashionable clothing INC
	个人名称: <b>Name and Phone</b>
	2:联系电话: <b>Name and Phone</b>
<b>EIN</b> →	3:资金来源:商业销售
	4:公司注册号码:92-3251373
	5:公司业务性质:服装饰品
	6:公司注册地址: 4031 university DR FL 2ND Fairfax VA 22030
	7: ssn 号码: <b>SSN</b>
	<b>交易信息</b>
	1:首次交易预期日: 06/06/2023
	2:交易的货币种类和预期交易额 : 38000USD
	3:预期月交易额: 100000USD
	4:预期年交易额: 1000000USD
	<b>银行信息</b>
	1:银行全称 : BANK OF AMERICA
	2:IBAN/Account Number: <b>1017</b>
	3:Routing Number : 051000017
	4:Swift/ABA/Sort Code :
	5:开户注册地址: 4031 university DR FL 2ND Fairfax VA 22030
	6:开户银行地址: 45470 Dulles Crossing plaza,Dulles,VA 20166
	7:开户国家 :USA
	8:公司营业执照复印件/个人 ID 复印件

- ii. A document containing; (1) detailed information about Bank-1 account number xxxxxxxx1017, (2) an apparent online banking username (containing J.D.'s name) with an apparent online banking password, (3) an email address (containing J.D.'s name) with an apparent password for this email account<sup>8</sup>, (4) the phone number associated with account number xxxxxxxx1017 in Bank-1 records, (5) SSN-1, and (6) a driver's license number ending in xxxx9136. An image of this document is displayed below:

```

Bank Name: BOA bank
Account Name: Kim fashionable clothing INC
Routing number: 051000017
Account number: [REDACTED] 1017
Address of the bank: 45470 Dulles Crossing plaza, Dulles, VA 20166
Company/Personal Address: 4031 university DR FL 2ND Fairfax VA 22030

online
ID: [REDACTED]
PW: Cal210038
mailbox
ID: [REDACTED]@gmail.com
PW: Cal210038

phone: [REDACTED]

ssn: [REDACTED] SSN

DL: [REDACTED] 9136

```

---

<sup>8</sup> The apparent passwords for the online banking account and the email account are both “Cal210038”. In my training and experience, it is common for fraudsters to reuse the same passwords for multiple accounts to make it easier for their co-conspirators to access the various accounts utilized in the scheme.



- iii. Multiple images of the IRS EIN document for Kim Fashionable Clothing Inc. One of these images is displayed below:

IRS DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
CINCINNATI OH 45999-0023

Date of this notice: 03-31-2023  
Employer Identification Number:  
92-3251373  
Form: 35-6  
Number of this notice: CP 575 A  
For assistance you may call us at:  
1-800-829-4933  
IF YOU WRITE, ATTACH THE  
STUB AT THE END OF THIS NOTICE.

KIM FASHIONABLE CLOTHING INC  
4031 UNIVERSITY DR PL 2ND  
FAIRFAX, VA 22030

WE ASSIGNED YOU AN EMPLOYER IDENTIFICATION NUMBER

Thank you for applying for an Employer Identification Number (EIN). We assigned you EIN 92-3251373. This EIN will identify you, your business accounts, tax returns, and documents, even if you have no employees. Please keep this notice in your permanent records.

Taxpayers request an EIN for their business. Some taxpayers receive CP575 notices when another person has stolen their identity and are opening a business using their information. If you did not apply for this EIN, please contact us at the phone number or address listed on the top of this notice.

When filing tax documents, making payments, or replying to any related correspondence, it is very important that you use your EIN and complete name and address exactly as shown above. Any variation may cause a delay in processing, result in incorrect information in your account, or even cause you to be assigned more than one EIN. If the information is not correct as shown above, please make the correction using the attached tear-off stub and return it to us.

Based on the information received from you or your representative, you must file the following forms by the dates shown.

Form 1120 04/15/2024

If you have questions about the forms or the due dates shown, you can call us at the phone number or write to us at the address shown at the top of this notice. If you need help in determining your annual accounting period (tax year), see Publication 538, *Accounting Periods and Methods*.

We assigned you a tax classification (corporation, partnership, etc.) based on information obtained from you or your representative. It is not a legal determination of your tax classification, and is not binding on the IRS. If you want a legal determination of your tax classification, you may request a private letter ruling from the IRS under the guidelines in Revenue Procedure 2020-1, 2020-1 I.R.B. 1 (or superseding Revenue Procedure for the year at issue). Note: Certain tax classification elections can be requested by filing Form 8832, *Entity Classification Election*. See Form 8832 and its instructions for additional information.

IMPORTANT INFORMATION FOR S CORPORATION ELECTION:  
If you intend to elect to file your return as a small business corporation, an election to file a Form 1120-S, U.S. Income Tax Return for an S Corporation, must be made within certain timeframes and the corporation must meet certain tests. All of this information is included in the instructions for Form 2553, *Election by a Small Business Corporation*.

- iv. A Texas driver's license in J.D.'s name. An image of this driver's license<sup>9</sup> is displayed below:



- v. A “Virtual Currency Purchase & Sale Agreement” between LI’s business Staring LLC and Kim Fashionable Clothing Inc.

36. The stack of printed documents described in paragraph 35.c, also contained a work kit for the business Universe Furniture LLC. This work kit contained documents similar to the documents described above for Kim Fashionable Clothing Inc. It also contained a printout of transactions from Universe Furniture LLC’s Bank-5 account. This printout shows inbound wire

---

<sup>9</sup> Records obtained from Bank-2 regarding account number xxxxxx9228 (referenced in paragraph 17) included an image of this same driver’s license.

transfers (from suspected victims for the benefit of Universe Furniture LLC) and outbound wire transfers to **LI's** business Staring LLC. An image of this printout is displayed below:

The screenshot shows a Chase Business credit card transaction history. The header includes navigation links: transfer, Collect & deposit, Investments, Account management, and Security. Below the header is a search bar with a dropdown menu set to 'All transactions' and a 'Search' button. The table below lists transactions with columns for Description, Type, and Amount.

Description	Type	Amount
DOMESTIC WIRE TRANSFER A/C: STARING LLC LAS VEGAS NV [REDACTED]	Outgoing wire transfer	-\$27,12
CREDIT VIA: CITIZENS BANK [REDACTED] REF: CHASE BNF=UNIVERSE FURNITURE LLC [REDACTED] 43FF	Incoming wire transfer	\$45,00
Transfer from CHK ...5520 transaction#: [REDACTED]	Account transfer	\$27,17
TRANSFER CREDIT B/O: PNC BANK NATIONAL ASSOCIATION [REDACTED]	Incoming wire transfer	\$19,72
DOMESTIC WIRE TRANSFER A/C: STARING LLC LAS VEGAS NV [REDACTED]	Outgoing wire transfer	-\$5
Transfer from SAV ...2566 transaction#: [REDACTED]	Account	\$

### G. Examination of Devices Seized from LI

37. Pursuant to a search warrant (Case No. 1:24-sw-158) authorized by the Honorable Lindsey R. Vaala on March 8, 2024, law enforcement examined the contents of several electronic devices seized from **LI's** residence. During the examination of an Alienware Aurora R10 computer (seized from **LI's** upstairs office) law enforcement located Personally Identifiable Information ("PII") of suspected identity theft victims, business documents, identification documents, EINs, and/or bank account information for at least 25 different entities (including

fictitious businesses previously referenced in this affidavit). In addition, during the examination of an iPhone seized from **LI**, law enforcement located Telegram messages relevant to this investigation (including communications with Individual-3 and Individual-4).

38. In a Telegram Chat with Individual-3, **LI** and Individual-3 discuss closed/blocked bank accounts and the need to open new bank accounts, Zelle and wire transfers (for the benefit of **LI**, Individual-3, and others), converting funds into foreign currency, and converting funds to cryptocurrency.

39. On July 31, 2023, (approximately three weeks after the victim-funded wire transfers between **LI**'s Staring LLC and the Kim Fashionable Clothing account opened using the identification of J.D.) during a discussion regarding exchanging money for another individual, **LI** told Individual-3 "Time out. This business is a little dangerous."

40. On August 16, 2023, Individual-3 asked **LI** "Besides the money from these scammers, have you ever transferred money to anyone else doing normal business besides me and Greg?" Based on my training and experience, I believe that these messages corroborate **LI**'s knowledge of (1) the illicit source of the funds moving through his bank accounts, (2) the unlawful nature of the financial transactions that he was conducting, and (3) the "danger" of continuing to conduct these transactions.

41. In a separate Telegram Group Chat (with Individual-3 and Individual-4), **LI** coordinates the movement of funds from the fictitious business Carson Truck Service Inc. of Alexandria, Virginia to Individual-4.

- a. On September 7, 2023, **LI** asks Individual-4 if he can make a wire transfer the following day and Individual-4 agrees. **LI** asks Individual-4 to verify a bank account to receive the funds. Individual-4 tells **LI** that he needs to find a new



account and states “If I don’t have it figured out by morning. I’ll take it and send you crypto.” **LI** replied, “It is best to give me the account now, my friend is going to sleep, and he will wire you as soon as he wakes up.” Individual-4 gave **LI** wire transfer instructions for an account in Individual-4’s name and stated “Send to me. I’ll figure it out”.

- b. On September 8, 2023, Individual-4 sent the following message to the group chat, “He sent 30k? Damn.” **LI**, Individual-3, and Individual-4 subsequently discuss converting the funds to cryptocurrency.
- c. On September 13, 2023, Individual-4 asked the group chat that included **LI**, “What was the purpose of the wire? [Bank-6] locked my account”.
- d. On September 14, 2023, Individual-4 sent the following message to the group chat, “Bank-6 has removed the 30k from my account. The citi bank this was sent from was fraud.” Individual-4 then asked **LI** “...How well did you know this guy” and “He was client?”
- e. On September 15, 2023, **LI** sent the following message<sup>10</sup> to the group chat:

Bank Name: Citibank Account Name: Carson truck service Inc ABA Routing  
number:254070116 Account number: [REDACTED] 4523 Address of the bank: 5001 WISCONSIN AVE  
NW WASHINGTON DC 20016 Company/Personal Address: 105 Oronoco st ste 300 Alexandria  
VA 22314 CITI US SWIFT CODE : CITI US 33 online ID:TOKEN ACCOUNT PW: mailbox ID:  
chao1953hungc@gmail.com PW: Cal210038 phone: 7036534828 ssn: [REDACTED] 3132 DL:  
C [REDACTED] 6532

---

<sup>10</sup> The password in this message (PW: Cal210038) is the same password that appeared in the work kit for Kim Fashionable Clothing Inc, as described in paragraph 35.c.ii.


42. A review of IC3 complaints identified a complaint filed by the National Elder Fraud Hotline on behalf of Victim-6. According to the complaint, Victim-6 sent \$34,150 to Bank-2 account number xxxxxxx4523 (Carson Truck Service Inc) on September 6, 2023 as the result of a tech support scam. As described in the above Telegram messages, **LI** attempted to facilitate the transfer of these funds to the bank account of Individual-4 in exchange for crypto currency.

43. Based on my training and experience, I believe that this change in methodology (from **LI** directly receiving fraud proceeds into his bank accounts to **LI** facilitating the transfer of fraud proceeds through a third party in exchange for crypto currency) corroborates **LI's** knowledge of the unlawful nature of his conduct and represents an attempt by **LI** to distance himself from the criminal activity described in this affidavit.

**CONCLUSION**

44. Based on the facts set forth herein, there is probable cause to believe that the **TARGET** has committed violations of 18 U.S.C. §1956(h) (Conspiracy to Commit Concealment Money Laundering). Accordingly, I respectfully request that a criminal complaint be issued charging the **TARGET** with violations of 18 U.S.C. §1956(h) (Conspiracy to Commit Money Laundering). In addition, I respectfully request that a warrant be issued for the arrest of the **TARGET**.

Respectfully submitted,



Adam Cowan  
Special Agent, Treasury Inspector General for  
Tax Administration

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1

by telephone on May 15, 2024:



Digitally signed by Ivan Davis  
Date: 2024.05.15 15:09:19 -04'00'

Honorable Ivan D. Davis  
United States Magistrate Judge  
Alexandria, Virginia

**ATTACHMENT A**

**Ziguang LI** is a 36-year-old Asian male with black hair and brown eyes. **LI** is 5'7" and weighs approximately 160 pounds.

